AUTOMATED DATA ENTRY METHOD AND SYSTEM

RELATED APPLICATIONS

[0001] The following U.S. patent is hereby incorporated by reference into the subject application as if set forth herein in full: (1) U.S. Patent No. 6,463,417, entitled "Method of Distributing Health Information".

FIELD OF THE INVENTION

[0002] This invention relates to automated data entry and, more particularly, to automated data entry within a medical records management system

BACKGROUND

[0003] Traditionally, the medical records of a patient are paper-based medical records, in which each medical service provider (that provides medical services to the patient) maintains a separate medical record for that patient.

[0004] Often, when treating patients who have certain medical conditions, it is advisable to routinely monitor various variables of that patient's condition. Examples of these conditions include those patients who are overweight, diabetic, or have hypertension; and examples of these variables include body weight, blood glucose levels, and blood pressure (respectively). Further, when monitoring these variables, the patient's medical record should be updated to include these monitored variables.

[0005] Unfortunately, with paper-based medical records, the medical service provider would need to manually review the medical records of each of their patients to determine which patients have these conditions. Additionally, these patients would have to be manually contacted so that their paper-based medical records could be manually updated.

[0006] Currently, paper-based medical records are slowly being converted into electronic, centrally-located databases that are accessible by various medical service

providers.

SUMMARY OF THE INVENTION

In one implementation, a data entry method includes, in a computer-based data record including a plurality of data fields, defining one or more data fields for which desired field data is to be acquired. A data source in possession of the desired field data is contacted, and the desired field data is received from the data source.

One or more of the following features may also be included. The computer-based data record may be updated to include the desired field data. The computer-based data record may be a medical record. The data source may be a patient and the medical record may define at least a portion of the medical history of the patient.

Contacting a data source may include authenticating the data source. Authenticating the data source may include requiring that the data source enter an electronic password, and receiving the electronic password. Authenticating the data source may include requiring that the data source speak a verbal password, and receiving the verbal password. Authenticating the data source may include requiring that the data source provide an authenticating digital certificate, and receiving the authenticating digital certificate.

Contacting a data source may include transmitting an email to the data source, and providing the data source with text-based instructions concerning the desired field data. Contacting a data source may include telephonically contacting the data source, and providing the data source with speech-based instructions concerning the desired field data.

The desired field data may concern a numeric range-based variable.

In another implementation, a data entry method includes, in a computer-based medical record including a plurality of data fields, defining one or more data fields for which desired field data is to be acquired. The medical record defines at least a portion of the medical history of a patient. The patient is telephonically contacted, and the desired

field data is received from the patient. The computer-based medical record is updated to include the desired field data.

[0007] The above-described methods may also be implemented as a sequence of instructions executed by a processor.

[0008] The details of one or more implementations is set forth in the accompanying drawings and the description below. Other features and advantages will become apparent from the description, the drawings, and the claims.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a diagrammatic view of record organization system coupled to a distributed computing network;

FIG. 2 is a more-detailed diagrammatic view of the record organization system of FIG. 1;

FIG. 3 is a diagrammatic view of a key maintenance module and a key processing module of the record organization system of FIG. 1;

FIG. 4 is a diagrammatic view of a key configuration display screen rendered by the record organization system of FIG. 1;

FIG. 5 is a block diagram of a record processing module of the record organization system of FIG. 1;

FIG. 6 is a diagrammatic view of a patient selection display screen rendered by the record organization system of FIG. 1; and

FIG. 7 is a diagrammatic view of a patient's medical record rendered by the record organization system of FIG. 1

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0009] Referring to FIG. 1, there is shown a record organization system 10 that manages the various access keys 12, 14, 16 possessed by a medical service provider 18.

Access keys 12, 14, 16 are provided to medical service provider 18 by various patients 20, 22, 24.

[0010] Record organization system 10 typically resides on and is executed by a computer 26 that is connected to network 28. Computer 26 may be a web server running a network operating system, such as Microsoft Window 2000 Server ™, Novell Netware ™, or Redhat Linux ™. Typically, computer 26 also executes a web server application, such as Microsoft IIS ™, Novell Webserver ™, or Apache Webserver ™, that allows for HTTP (i.e., HyperText Transfer Protocol) access to computer 26 via network 28.

[0011] The instruction sets and subroutines of record organization system 10, which are typically stored on a storage device 30 coupled to computer 26, are executed by one or more processors (not shown) and one or more memory architectures (not shown) incorporated into computer 26. Storage device 30 may be, for example, a hard disk drive, a tape drive, an optical drive, a RAID array, a random access memory (RAM), or a read-only memory (ROM).

[0012] As will be explained below in greater detail, a patient (e.g., patient 20) typically provides an access key (e.g., key 12) to medical service provider 18 through a patient computer 32, which is also connected to network 28. Additionally, medical service provider 18 accesses record organization system 10 through a client computer 34.

[0013] Referring also to FIG. 2, record organization system 10 includes a centralized key repository 50 and a centralized medical records repository 52. Additionally, record organization system 10 includes a key maintenance module 54, a key processing module 56, and a record processing module 58, each of which will be discussed below in greater detail.

[0014] Centralized medical records repository 52 allows for the centralized storage of medical records 60, 62, 64 concerning various patients 20, 22, 24 respectively. As disclosed in U.S. Patent No. 6,463,417, medical records 60, 62, 64 are typically divided into portions or levels, in that certain portions are considered more confidential than other

portions. For example, a portion / level of the medical record that may be considered the least confidential might include general patient identification information and information concerning the patient's blood type and allergies. A portion / level of a medical record that may be considered to have an intermediate level of confidentiality might include information concerning the serological data, psychiatric data, cardiology data, and genetic data. A portion / level of the medical record that may be considered highly confidential may include infectious disease (e.g., HIV, and sexually transmitted diseases) data.

[0015] This specific assignment of confidentiality levels and the apportionment of the medical record into various portions / levels is for illustrative purposes only and is not intended to limit the scope of this disclosure.

[0016] Medical records 60, 62, 64 may be incrementally generated / configured online by the various medical service providers that provide care to patients 20, 22, 24. Alternatively, existing medical records may be uploaded (i.e., transferred) to medical records repository 52 from a remote storage location (not shown).

[0017] Referring also to FIG. 3, patients 20, 22, 24 use key maintenance module 54 to generate 100 access keys 12, 14, 16 that grant access to various portions of the respective medical records 60, 62, 64. Accordingly, though the use of key maintenance module 54, the patient can generate access keys that not only regulate who has access to their medical records, but also regulate the level of access (i.e., which portions of a patient's medical record are viewable by the medical service provider to which the key is provided). Examples of access keys 12, 14, 16 are passwords (that allow access to various portions of a medical record) and decryption keys (that decrypt various portions of an encrypted medical record).

[0018] Typically, key maintenance module 54 is a web-enabled application that is accessed by the patients (e.g., patient 20) through a browser application (e.g., Microsoft Internet Explorer ^{tm}, or Netscape Navigator ^{tm}) that is running on patient computer 32, and the patient logs into record organization system 10 using an encrypted SSL (i.e., secure

sockets layer) connection. Alternatively, key maintenance module 54 may be a local application that is executed locally on patient computer 32.

[0019] As stated above, key maintenance module 54 allows a patient to generate 100 an access key for a specific medical service provider that grants, to that medical service provider, a defined level of access to that patient's medical records. Once this access key is generated, the access key is transmitted 102 to the medical service provider 18. This transmission of the access key may be implemented by transferring the access key from the patient to the medical service provider. This may occur by attaching the access key to an email that is transmitted to the medical service provider. Once received, the medical service provider may then transfer the newly-generated key to the key processing module 56 (to be discussed below in greater detail) of the record organization system 10. Alternatively, the patient may directly transfer the newly-generated key to the key processing module 54 of the record organization system 10.

[0020] Regardless of the manner in which the patient transfers the access key to the medical service provider, the access key will ultimately be received 104 by key processing module 56, which receives any access keys (e.g., keys 12, 14, 16) generated and transmitted by patients 20, 22, 24. Once these keys are received 104, they are stored 106 on centralized key repository 50. Additionally, if record organization system 10 is servicing multiple medical service providers (e.g., medical service providers 17, 18, 19), the received keys are associated 108 with the appropriate medical service provider so that the keys transmitted to a first provider are not available to a second provider.

[0021] Referring also to FIG. 4, when a patient is generating an access key (e.g., access key 14) for a medical service provider, key maintenance module 54 provides the patient (e.g., patient 22) with a rendered screen display 120 that allows the patient to select one or more access parameters 122 that define the access level granted to that particular medical service provider. Display 120 identifies the patient (i.e., Timothy Smith; patient 22) and allows the patient to select the recipient 124 of the access key being generated by the

patient. In this example, the recipient 124 is Family Medical Clinic; i.e., medical service provider 18.

[0022] As stated above, medical records 60, 62, 64 are typically divided into portions or levels, such that certain portions are considered more confidential than other portions. The access parameters 122 selected (i.e., checked) by the patient define the various portions of the patient's medical record that the medical service provider is going to have access to. In this particular case, the access key being generated by patient Timothy Smith (i.e., patient 22) for the Family Medical Clinic (i.e., medical service provider 18) is going to allow the medical service provider to access only two portions of the patient's medical record, namely the general portion and the psychiatric data. As the remaining access parameters are unchecked, medical service provider 18 is going to be prohibited from accessing any other portion of the patient's medical record. When generating the access key, the patient selects the appropriate access parameters 122 using a mouse pointer 126 (or some other pointing device, not shown).

[0023] Referring also to FIG. 5, when medical records are initially received, initially generated, and/or edited, record processing module 58 stores 140 the medical record on centralized medical record repository 52. Typically, medical record repository 52 is a database that allows for the organized storage and retrieval of the medical records 60, 62, 64.

[0024] Once these medical records are stored on medical record repository 52, record processing module 58 allows the medical service provider 18 to access 142 the medical records 60, 62, 64 stored on medical records repository 52. However, the medical service provider 18 is only given access to the portions of the medical records for which the medical service provider 18 possesses the appropriate key. For example, assume that medical service provider 18 is a medical clinic that provides an array of medical services to its patients. Further, assume that patient 20 uses medical service provider 18 for all of their

medical needs; patient 22 uses medical service provider 18 solely for treatment of depression; and patient 24 uses medical service provider 18 solely for treatment of HIV.

[0025] Concerning the access keys generated by each of these patients for medical service provider 18: patient 20 would typically provide medical service provider 18 with an access key (i.e., key 12) that grants access to their entire medical record; patient 22 would typically provide medical service provider 18 with an access key (i.e., key 14) that grants access to the general and psychiatric portions of their medical record; and patient 22 would typically provide medical service provider 18 with an access key (i.e., key 16) that grants access to the general and infectious disease portions of their medical record.

[0026] Record processing module 58 is typically a web-enabled application that is accessed by the medical service provider 18 through a browser application (e.g., Microsoft Internet Explorer ™, or Netscape Navigator ™) that is running on client computer 34. Typically, medical service provider 18 logs into record organization system 10 using an encrypted SSL (i.e., secure sockets layer) connection.

[0027] Referring also to FIG. 6, when accessing record organization system 10, record processing module 58 provides the medical service provider 18 with a rendered screen display 160 that includes a list of patient identifiers 162. Patient identifiers 162 define the particular patient(s) who provided access keys to medical service provider 18 (i.e., granting medical service provider 18 access to various portions of their medical record(s)). The patient identifiers 162 may be any element that uniquely identifies the patient, such as the patient's name, the patient's social security number, or a unique patient number. In this particular example, Mary Jones is patient 20, Timothy Smith is patient 22 (as stated above), and James Greco is patient 24.

[0028] The presence of each of these names in the list of patient identifiers 162 indicates that a key was received from that patient. In order to access the medical record of a patient for which the medical service provider has an access key (i.e., for one of the patients listed in the list of patient identifiers 162), the medical service provider 18 selects

the appropriate identifier using a mouse pointer 164 (or some other pointing device, not shown). For example, if the medical service provider wanted to access the medical record of Timothy Smith (i.e., patient 22), medical service provider 18 would typically double click (using a mouse) on the specific identifier 166 associated with Timothy Smith. Record processing module 58 would then, in turn, use access key 14 to access (i.e., retrieve, decrypt, and display) medical record 62, the medical record of Timothy Smith, i.e., patient 22.

[0029] Referring also to FIG. 7, medical record 62 may be displayed in a separate window or displayed full screen on the display of client computer 34. As discussed above, the key provided to the medical service provider 18 only allows access to the portion(s) of the patient's medical record that the patient wishes to allow access. As discussed above, Timothy Smith (i.e., patient 22) is being treated by medical service provider 18 for depression and access key 14 grants access to the general and psychiatric portions of Timothy Smith's medical record.

[0030] However, access key 14 does not permit access (i.e., prohibits access) to the other portions of Timothy Smith's medical record, namely Allergies, Serological Data, Cardiology Data, Genetic Data, and Infectious Disease Data. Accordingly, these portions of the patient's medical record are unavailable.

[0031] Medical records (e.g., medical record 62) are typically database records 180 that define general patient data through the use of various data fields (e.g., data field 182), each of which includes a field name 184 and a field value 186. Field value 186 may define an amount (e.g., a patient's systolic pressure) or a binary condition (e.g., whether or not a patient is a smoker). Additionally, as discussed above, the medical records include allergy data 188, serological data 190, psychiatric data 192, cardiology data 194, genetic data 196, and infectious disease data 198, each of which may be further broken down into data fields.

[0032] Through the use of record processing module 58, the medical service provider 18 may configure record organization system 10 so that selected data fields (e.g., data field

182) within a patient's medical record (e.g., medical record 62) may be automatically populated with desired field data obtained from the patient / trusted third party (e.g., a spouse, parent, or private nurse, for example), herein after a data source.

[0033] Referring again to FIG. 5, if a patient has a condition that requires medical supervision, it may be desirable for the medical service provider to define certain data fields within the medical record of that patient as data fields that need to be populated in the future, either on a one-time or a recurring basis.

[0034] For example, if a patient is seeing a medical service provider for treatment of hypertension, it may be desirable for the medical service provider to update the medical record of the patient to include weekly systolic and diastolic blood pressure readings. Further, if a patient is seeing a medical service provider for dietary reasons and the medical service provider places that patient on a diet, it may be desirable to update the medical record of the patient to include weekly or monthly weight measurements.

[0035] Accordingly, if desired 144, record processing module 58 allows the medical service provider 18 to define 146 one or more data fields (e.g., data field 182) within a patient's medical for which desired field data (e.g., the patient's diastolic pressure) is to be acquired. When defining the data field(s) to be automatically populated/updated, the medical service provider may define the populate/update procedure as a one-time event, or a recurring event. For example, the medical service provider may only be interested in obtaining the weight of a patient once (e.g., three months after the start of a diet). However, if a patient is suffering from chronic hypertension, the medical service provider may be interested in obtaining blood pressure readings on a monthly, weekly, or daily basis. Accordingly, when defining 146 the data field(s) for which field data is to be obtained, the date, time, and frequency of the event is also defined.

[0036] Once the field(s) are properly defined, at the scheduled date and time, the data source is contacted 148. Contacting the data source may include transmitting 150 an email or other electronic message to the data source, and providing 152 the data source with

text-based instructions concerning responding. Alternatively, the data source may be contacted telephonically 154 , and provided 156 with speech-based instructions concerning responding.

[0037] Examples of these instructions include a text or speech-based greeting such as "Hello, the is the Family Medical Clinic. We are calling to obtain your latest diastolic blood pressure reading".

[0038] Once initial contact is made with the data source, the data source is authenticated 158 (to confirm the identity of the data source), such that the authentication method varies depending on the type of contact made with the data source.

[0039] If the data source was contacted via email, the authentication process may require the data source to transmit 160 a password or PIN (i.e., personal identification number), which is subsequently received 162 by the medical service provider. This password or PIN may be included in the email response that the data source provides to the medical service provider. Alternatively, the data source may be required to provide 164 a digital certificate with their email response, which is subsequently received 166 by the medical service provider.

[0040] As is known in the art, a digital certificate is a file that identifies the user (i.e., in this situation, the data source) and include a copy of the user's public encryption key.

[0041] If the data source was contacted via the telephone, the authentication process may require that the data source enter 168 a password or PIN, which is subsequently received 170 by the medical service provider. Entry of the password / PIN may be accomplished through the use of the keypad on the patient's telephone. Alternatively, a verbal password / PIN may be used, in which the data source speaks 172 the password / PIN and voice recognition software (not shown) incorporated into the record organization system 10 receives 174 and analyzes the data source's spoken word to provide authentication.

[0042] Once authenticated, the data source enters and transmits the desired field data,

which is subsequently received 176 by record processing module 58. Again, the manner in which the data source enters and transmits the desired field data varies depending on the manner in which the data source was contacted. As above, the desired field data may be incorporated into an email, spoken into the telephone, or entered into the telephone via the telephone keypad. Once received, the desired field data is used to update 178 the medical record of the patient. This updating procedure may overwrite the old field data, or may enter the new field data as a chronological entry, thus allowing for historical tracking of the field data.

[0043] While the centralized key repository 50 and the centralized medical record repository 52 are described above as being located on a remote server, other configurations are possible. For example, as is known in the art, one or more of these repositories may be distributed across multiple computers / servers.

[0044] A number of implementations have been described. Nevertheless, it will be understood that various modifications may be made. Accordingly, other implementations are within the scope of the following claims.